

RESUMEN DE SOLUCIÓN

Cloudflare One for Data Protection

Mejora tu arquitectura de red para una protección de datos más eficaz, más productiva y más ágil.

Protección unificada para datos, en todas partes

Los nuevos riesgos en protección de datos exigen una seguridad moderna

Hoy en día, el volumen, la variedad y la velocidad de los datos han crecido exponencialmente, y las organizaciones se enfrentan a riesgos cada vez mayores derivados de:

Los entornos de nube y SaaS en expansión
↳ incluidas las nuevas herramientas de IA cuestionables como ChatGPT
↳ que conducen a la exposición de código fuente valioso

La suite de protección de datos de Cloudflare One se ha creado para estar a la vanguardia de estos riesgos modernos.

La consolidación de soluciones específicas en una única plataforma y red permite a Cloudflare ofrecer una protección de datos que es:

- **Más eficaz**, ya que simplifica la conectividad y la gestión de políticas.
- **Más productiva**, al garantizar experiencias de usuario rápidas, fiables y coherentes en todas partes.
- **Más ágil**, gracias a su capacidad para innovar rápidamente y satisfacer tus nuevos requisitos de seguridad.



Un servicio de seguridad en el perímetro (SSE) para proteger los datos en la web, las aplicaciones SaaS y las aplicaciones privadas

Implementa Cloudflare de manera progresiva en tu recorrido SSE para:

1. Proteger el acceso a los datos con Zero Trust
2. Detener amenazas como el phishing y el ransomware
3. Detectar y proteger tu información más confidencial

Resuelve por los riesgos cada vez mayores para la protección de los datos...

Huella SaaS en expansión

El 82 %

de las fugas de datos se produjeron en entornos de nube.[1]

Y, por supuesto, los costes asociados a las mismas siguen aumentando, en concreto, un 15 % en los últimos 3 años.[1]

Nuevas regulaciones diferentes

El 71 %

de los países disponen de normativas para proteger los datos y la privacidad.[2]

En EE. UU., **11 estados** cuentan ahora con leyes exhaustivas en materia de protección de datos, frente a los 3 de 2021.[3]

Transformación digital

El 89 %

de los CISO afirma que avanzar rápido con las iniciativas de transformación digital plantea riesgos imprevistos en la seguridad de los datos de la empresa.[4]

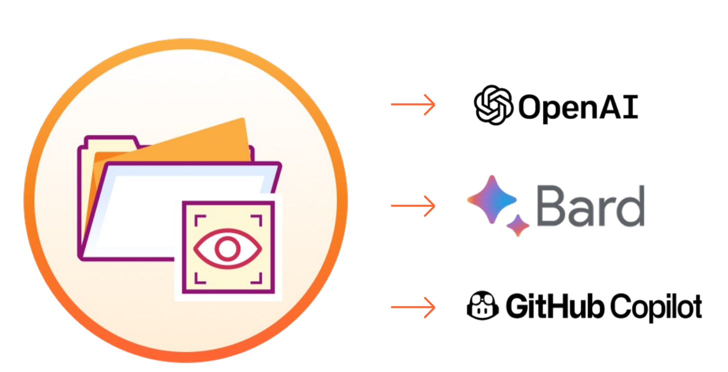
Caso de uso nº 1: Proteger el código de los desarrolladores

Problema
El código puede quedar expuesto o ser objeto de robo en muchas herramientas para desarrolladores, incluso en lugares a la vista, como repositorios públicos.

Solución
Analiza y corrige los repositorios públicos mal configurados, como GitHub, que corren el riesgo de sufrir fugas de código. Detecta el código fuente en cargas/descargas y aplica controles.



Caso de uso nº 2: Visibilidad de la exposición de datos y gestión de riesgos



Problema
Los datos abarcan diversos entornos SaaS y en la nube, elementos de Shadow IT no autorizados y herramientas de IA emergentes como ChatGPT, lo que aumenta el riesgo de fugas.

Solución
Analiza las suites SaaS en busca de configuraciones erróneas con detecciones que incluyan tecnología DLP para datos confidenciales. Aumenta la visibilidad del uso de aplicaciones no autorizadas y, a continuación, permite, bloquea, aísla o aplica controles Zero Trust para acceder a ellas.

Caso de uso nº 3: Cumplir la normativa

Problema
Requisitos legales cada vez más estrictos para que las empresas garanticen la seguridad y la privacidad de los datos, incluidas sanciones mayores por incumplimiento.

Solución
Identifica y aplica controles a las clases de datos regulados (información de identificación personal, información sanitaria, datos financieros). Mantén informes de auditoría detallados mediante registros y análisis SIEM más exhaustivos. Reduce la superficie de ataque con una postura de seguridad integral Zero Trust.



Cómo funciona



Una plataforma unificada

Cloudflare unifica la visibilidad y los controles de DLP, CASB, ZTNA, SWG, RBI y los servicios de seguridad del correo electrónico en una única plataforma para simplificar la gestión.

Una red programable

Un plano de control con servicios creados en nuestra propia plataforma para desarrolladores para aplicar controles a los datos en tránsito, en uso y en reposo en todos los puntos de aplicación: entornos web, aplicaciones SaaS o aplicaciones privadas.

Ejemplo de medidas de control con servicios componibles

Implementación de la prevención de pérdida de datos (DLP) para datos en tránsito y acceso seguro

- Busca datos confidenciales en el tráfico y los archivos, y configura políticas de bloqueo con DLP.
- Descubre y gestiona los elementos de Shadow IT con CASB.
- Protege el acceso a los datos en las aplicaciones con ZTNA.
- Bloquea a los inquilinos personales de aplicaciones SaaS para evitar la filtración de datos.

Aislamiento de las aplicaciones para proteger los datos en uso

- Bloquea los comandos copiar/pegar, cargar/descargar, imprimir, entradas de teclado... todo ello sin un cliente de dispositivo.
- La implementación sin cliente es perfecta para dispositivos no administrados, usuarios de terceros y herramientas de IA como ChatGPT.
- Aplica políticas DLP dentro de aplicaciones aisladas.

Protección de los datos en reposo en las aplicaciones SaaS

- Analiza las aplicaciones SaaS en busca de actividades sospechosas, configuraciones erróneas y datos confidenciales.
- Adopta medidas prescriptivas para solucionar los riesgos mediante políticas SWG.

Integración para optimizar la conformidad y los controles

- Envío de registros a tu SIEM preferido para correlación y auditoría.
- Integración con 18 de las suites SaaS más populares para análisis CASB basados en API.
- Sincronización continúa con las etiquetas de Microsoft Information Protection (MIP) para tus políticas DLP.

Mayor protección de datos con Cloudflare



Más eficaz, ***ya que reduce la complejidad***

Simplifica la conectividad con muchas opciones flexibles para enviar tráfico a Cloudflare para su aplicación.

Utiliza análisis basados en API para las suites SaaS o modos sin cliente para ZTNA y RBI a fin de proteger el acceso a las aplicaciones. Para el reenvío del proxy que dirige el tráfico, utiliza un cliente de dispositivo o accesos de red de área amplia en todos los servicios de seguridad.



Más productiva , ***ya que mejora la experiencia del usuario***

Nuestra red está en todas partes, lo que garantiza que los controles se apliquen con una inspección de paso único cerca de los usuarios finales y los datos, estén donde estén.

La aplicación de controles de datos que nunca interrumpan el trabajo garantizan experiencias de usuario fiables y poco intrusivas. Se ha demostrado que nuestra solución es más rápida que la de otros proveedores de SSE.



Más ágil, ***gracias a su capacidad para innovar rápidamente***

Nuestra arquitectura de red programable nos permite crear capacidades a gran velocidad, para que puedas adaptarte a los nuevos riesgos con agilidad.

Adoptamos rápidamente nuevas normas y protocolos de seguridad (como conexiones solo IPv6 o cifrado HTTP/3) para garantizar la actualización de la protección de datos.

Qué dicen nuestros clientes

"En la actualidad, Cloudflare One ayuda a evitar que nuestros usuarios compartan código y datos confidenciales con herramientas como ChatGPT y Bard, lo que nos permite aprovechar la IA de forma segura [...]. De cara al futuro, estamos entusiasmados con las continuas innovaciones de Cloudflare para proteger los datos y, en particular, con su visión y hoja de ruta para servicios como DLP y CASB".

Tanner Randolph
CISO

Applied Systems
Leer caso práctico

Otros casos prácticos

- **Empresa de gas natural de la lista Fortune 500:** proteger el acceso de los proveedores a los datos
- **Importante centro de empleo de EE. UU.:** proteger el código y la información personal
- **Aerolínea regional de EE. UU.:** mitigar los riesgos de exposición de datos de clientes
- **Empresa sanitaria australiana:** proteger datos médicos regulados
- **Fabricante estadounidense de dispositivos médicos:** facilitar la conformidad con la HIPAA

Vías de adopción habituales

Fase 1: Proteger los datos en la web y las aplicaciones SaaS

- Detecta el intercambio de datos y el acceso indebido de usuarios en aplicaciones SaaS
- Detecta el uso de aplicaciones SaaS autorizadas y no autorizadas
- Detecta y controla los datos confidenciales que entran en cualquier aplicación SaaS
- Aísla las amenazas de salida de datos confidenciales de las aplicaciones SaaS

Fase 2: Proteger los datos en aplicaciones privadas

- Protege el acceso a aplicaciones privadas / en la nube autoalojadas y aplica controles de datos
- Aísla las amenazas de salida de datos confidenciales de las aplicaciones privadas

Primeros pasos

APRENDE...

los riesgos cada vez mayores para la protección de los datos en esta infografía

ENTIENDE...

el funcionamiento de la plataforma en esta demostración

COMPRUEBA...

el valor solicitando un seminario con expertos

1. Cost of a Data Breach Report 2023, IBM
2. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
3. Asociación internacional de profesionales de la privacidad (IAPP)
4. Informe "State of the CISO" 2023